### *Remarks*

The present claim amendments and cancellations are submitted pursuant to the examiner's comments in the non-final office action letter dated March 13, 2007. These amendments and cancellations are entered in order to place the claims into condition for allowance in view of said examiner's letter. However, applicants are not conceding in this application that claims 1-35 as originally submitted are not patentable over the prior art of record, and the present amendments and cancellations are made only for facilitating expeditious prosecution of other subject matter believed to be allowable in view of the examiner's letter of March 13, 2007. Applicants respectfully reserve the right to pursue any of the originally submitted claims 1-35, as well as other claims, in one or more continuations and/or divisional patent applications.

### *Claim Rejections 35 USC § 101*

Claims 11-24 stand rejected under 35 USC § 101 because they are not tangible embodiments of a claimed invention.

Claim 11 has been amended to claim a *memory device* comprising a table containing at least one characteristic and a set of state code, and a *processor means* in communication with the memory device configured to examine received packets flowing within computer network communications for the triplet. Thus claim 11 as amended now claims tangible system devices believed allowable under 35 USC § 101. Claims 12-13 and 16-19 are directly or indirectly dependent upon amended claim 11, and thus incorporate all of its limitations: they are thus each also believed allowable under 35 USC § 101. Claims 14 and 15 have been cancelled.

Claim 20 has been amended to claim a computer-*readable* medium pursuant to the examiner's comments, and is thus now believed to claim a tangible article allowable under 35 USC § 101. Claim 21-22 are directly or indirectly dependent upon amended claim 20, and thus incorporate all of its limitations: they are thus each also believed allowable under 35 USC § 101. Claims 23 and 24 have been cancelled.

***Claim Rejections 35 USC § 102***

Claims 1, 2, 5, 6, 8, 11, 12, 14-18, 20-31, 34 and 35 stand rejected under 35 USC § 102(e) as being anticipated by Shanklin et al. (U.S. Pat. No. 6487666). Prior art is anticipatory only if every element of the claimed invention is disclosed in a single item of prior art in the form literally defined in the claim. Jamesbury Corp. v. Litton Indus. Products, 756 F.2d 1556, 225 USPQ 253 (Fed. Cir. 1985); Atlas Powder Co. v. du Pont, 750 F.2d 1569, 224 USPQ 409 (Fed. Cir. 1984); American Hospital Supply v. Travenol Labs, 745 F.2d 1, 223 USPQ 577 (Fed. Cir. 1984)

Claims 1, 2, 8, 25-26, 30 and 34. Independent method claim 1 has been amended to claim a method for monitoring network communications for a *specifically defined predefined sequential* ***triplet*** of TCP/IP protocol set packets, the triplet (1) an *initial SYN* packet originating from a source address, (2) a *next sequential SYN/ACK* packet issuing from a target device address *in response to* the SYN packet, and (3) a *last sequential RST packet* originating from the *source address* in response to the SYN/ACK packet, wherein a unauthorized scanning alert is issued an ***if*** the predefined sequence of packets are each relevant to the *source address*. Recognition of this specifically claimed triplet as useful in identifying unauthorized scanning is novel and not taught by Shanklin et al. *in the form literally defined in the claim.* Shanklin et al is unambiguously silent on the significance of the triplet and instead teaches observing a frequency of SYN packet transmissions. Thus amended claim 1 is clearly allowable over Shanklin et al. under 35 USC § 102(e) as established by the clear case teachings above. Claims 2 and 8 are directly dependent upon amended claim 1 and thus incorporate all of its limitations: they are thus each also believed allowable over Shanklin et al. under 35 USC § 102(e) for the same reasons.

Independent method claims 25 and 30 have also been amended to claim methods having step elements analogous to those discussed above with respect to amended claim 1, wherein alerts are issued if the predefined sequential protocol triplet is observed, and their specific claim elements are not taught by Shanklin et al., amended claims 25 and 30 are also believed allowable over Shanklin et al. under 35 USC § 102(e). Claim 26 is directly dependent upon amended claim 25, and claims 34 and 35 are directly or

indirectly dependent upon amended claim 30, and thus each incorporate all of their respective limitations and are also believed allowable over Shanklin et al. under 35 USC § 102(e).

Claims 11, 12, and 16-18. Independent system claim 11 has been amended to claim an intrusion detection system analogous to the method claimed by amended claim 1, wherein a memory device comprises a table containing at least one characteristic identifying network devices and a set of state code corresponding to a sequence in which the predefined sequential triplet of TCP/IP protocol packets are observed, and a processor means in communication with the memory device is configured to examine computer network for the triplet and responsively adjust the state code and generate an alert. Again, each of these specifically claimed system elements are not taught by Shanklin et al., and amended claim 11 is clearly allowable over Shanklin et al. under 35 USC § 102(e). Claims 12 and 16-18 are directly or indirectly dependent upon amended claim 11 and thus incorporate all of its limitations: they are thus each also believed allowable over Shanklin et al. under 35 USC § 102(e) for the same reasons.

Claims 20-22. Independent article of manufacture claim 20 has been amended to claim a computer-readable medium comprising computer instructions which, when executed on a computer processing means, cause the means to perform specific steps analogous to method steps claimed by amended claim 1 and not taught by Shanklin et al., and amended claim 20 is allowable over Shanklin et al. under 35 USC § 102(e) for the reasons discussed with respect to amended claims 1 and 11. Claims 21 and 22 are directly or indirectly dependent upon amended claim 20 and thus incorporate all of its limitations: they are thus each also believed allowable over Shanklin et al. under 35 USC § 102(e) for the same reasons.

Claims 5, 6, 14, 15, 23, 24 and 31 have been cancelled, and their rejection thus rendered moot. No further response or action by applicants is believed required to this rejection.

***Claim Rejections 35 USC § 103***

Applicants hereby acknowledge their obligation to inform the United States Patent and Trademark Office if the subject matter of any claims before the examiner is not commonly owned.

Claims 7, 9, 10, 13, 19, 32 and 33 stand rejected under 35 USC § 103(a) as being unpatentable over Shanklin et al. The law is quite clear that in order for a claimed invention to be rejected on obviousness, the prior art must *suggest* the modifications sought to be patented; In re Gordon, 221 U.S.P.Q. 1125, 1127 (CAFC 1984); ACS Hospital System, Inc. v. Montefiore Hospital, 221 U.S.P.Q. 929, 933 (CAFC 1984). The foregoing principle of law has been followed in Aqua-Aerobic Systems, Inc. v. Richards of Rockford, Inc., 1 U.S.P.Q. 2d, 1945 (D.C. Illinois 1986). In the Aqua-Aerobic's case, the Court stated that the fact that a prior reference *can be modified* to show the claimed invention does *not* make the modification obvious unless a prior reference *suggests* the desirability of the modification.

In In Re Oetiker, 24 U.S.P.Q. 2nd 1443, 1445 (CAFC 1992) held:

> "There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge can not come from the applicant's invention itself."

Most significantly, the CAFC in the case of In Re Dembiczak, 50 U.S.P.Q.2nd 1614 (CAFC 1999) held at 1617:

> "…(examiner can satisfy burden of obviousness in light of combination 'only by showing some objective teaching [leading to the combination]');"

Thus, it is clear that where an individual reference does not teach the entire invention, then the modification which the invention represents must be suggested and motivated by some other reference through some objective teaching and cannot come from the application itself, which is not the case here since there is but one reference cited.

More specifically, dependent claim 7 and intervening dependent claims 5 and 6 have been cancelled and their subject matter restated and incorporated, with additional claim elements, into amended independent claim 1. As discussed above with respect to the 35 USC § 102 rejection of claim 1, amended claim 1 now claims a method for monitoring network communications for a *specifically defined predefined sequential* ***triplet*** of TCP/IP protocol set packets, the triplet (1) an *initial SYN* packet originating from a source address, (2) a *next sequential SYN/ACK* packet issuing from a target device address *in response to* the SYN packet, and (3) a *last sequential RST packet* originating from the *source address* in response to the SYN/ACK packet, wherein a unauthorized scanning alert is issued an ***if*** the predefined sequence of packets are each relevant to the *source address*.

In his letter of March 12, 2007 at paragraph 16, the examiner states that recognition of the significance of this triplet would be obvious, for example asserting that the triplet is a "common set of up of TCP/IP three-way handshaking." However, the examiner's contention is unsupported: there is no citation to Shanklin et al. for such teachings, nor to any *specific* modifying prior art citation to supply the *specific* modification. In fact, applicants specification as originally filed establishes that the triplet is unambiguously ***not*** a common handshake protocol familiar to one skilled in the art, at paragraph 0035 of the published application:

> ...This sequence of packet SYN, SYN/ACK and RST1 when detected in the recited sequence by the detection device in the target would very likely indicate that malicious scanning is being conducted in the network. The preventative measures set forth herein is practiced once this illegal sequence of packets are observed. It should be noted that ***if*** the scanner was a ***legitimate*** device on the network, then after receiving SYN/ACK from the target ***it would issue the flow labeled Acknowledge (ACK)***. *The flow's* ***SYN, SYN/ACK and ACK are legitimate TCP handshaking signals*** *that are exchanged in order to establish a legitimate session between stations on the network.*

Thus recognition of the specifically claimed triplet of amended claim 1 as useful in identifying unauthorized scanning is novel and not taught by Shanklin et al., nor would one skilled in the art use common TCP/IP protocol teachings to modify Shanklin et al to teach the invention claimed by amended claim 1. Instead teachings as to the invention specifically

claimed by amended claim 1 come only from applicant's own specification, and thus rejection of amended claim 1 under 35 USC § 103(a) as being unpatentable over Shanklin et al is clearly impermissible, and in particular pursuant to *In Re Oetiker* and *In Re Dembiczak.* Thus amended claim 1 is clearly allowable over Shanklin et al. under 35 USC § 102(e) as established by the clear case teachings above.

Claims 2-4 and 8-10 are directly dependent or indirectly upon amended claim 1 and thus incorporate all of its limitations: they are thus each also believed allowable over Shanklin et al. under 35 USC § 103(a). As discussed above independent method claims 25 and 30 have also been amended to claim methods having step elements analogous to those discussed above with respect to amended claim 1, and amended claims 25 and 30 are also believed allowable over Shanklin et al. under 35 USC § 103(a) for the same reasons as established in the above discussion of amended claim 1. Claim 26 is directly dependent upon amended claim 25, and claims 34 and 35 are directly or indirectly dependent upon amended claim 30, and thus each incorporate all of their respective limitations and are also believed allowable over Shanklin et al. under 35 USC § 103(a).

As discussed above independent system claim 11 has been amended to claim an intrusion detection system analogous to the method claimed by amended claim 1 and is thus also believed allowable over Shanklin et al. under 35 USC § 103(a) for the same reasons as established in the above discussion of amended claim 1. Claims 12-13 and 16-19 are directly or indirectly dependent upon amended claim 11 and thus incorporate all of its limitations, and they are also believed allowable over Shanklin et al. under 35 USC § 103(a) for the same reasons.

Amended independent article of manufacture claim 20 claims a computer-readable medium comprising computer instructions which, when executed on a computer processing means, cause the means to perform specific steps analogous to method steps claimed by amended claim 1 and is thus also believed allowable over Shanklin et al. under 35 USC § 103(a) for the reasons discussed with respect to amended claims 1. Claims 21 and 22 are directly or indirectly dependent upon amended claim 20 and thus incorporate all of its limitations: they are thus each also believed allowable over Shanklin et al. under 35 USC § 103(a) for the same reasons.

Claims 3 and 4 stand rejected under 35 USC § 103(a) as being unpatentable over Shanklin et al in view of Etheridge et al. (US Patent Publication No. 2004/0054925). However, the examiner cites to Etheridge et al. for teachings with respect to histogram-related limitation teachings in claims 3 and 4. Claims 3 and 4 depend directly and indirectly, respectively, upon amended claim 1 and thus incorporate all of its limitations. As Etheridge et al. is not cited for the proposition that it teaches the inventions specifically claimed in amended claim 1, as more fully discussed above, claims 3 and 4 are thus each also believed allowable over Shanklin et al. in view of Etheridge under 35 USC § 103(a).

***Conclusion***

Claims 5-7, 14-15, 23-24, 27-29, and 31-33 have been cancelled and the issues raised by the examiner with respect to their rejection under 35 USC § 102 or § 103 are now moot. No further response or action by applicants is believed required to this rejection.

The present claim amendments are believed to clarify the scope of the inventions claimed as distinguishable and patentable over the prior art of record, and claims 1-4, 8-13, 16-22, 25-26, 30 and 34-35 are now believed in condition for allowance pursuant to the examiner's letter of March 12, 2007. Early issuance of the appropriate notification of allowance is respectfully requested. The examiner is also encouraged to telephone the undersigned if any further clarifications or examiner's amendments are required to accomplish the issuance of a notice of allowance or otherwise further the case.

Respectfully submitted,

Date: May 30, 2007

Patrick J. Daugherty, Reg. No. 41,697
CUSTOMER NO. 26675